IN THE CLAIMS:

Please cancel Claim 1 without prejudice.

Please add new Claim 2 as follows:

--2. A method of managing encryption keys in a cryptographic co-processor, which comprises the steps of:

selecting a key type from one of a symmetrical key type and an asymmetrical key type, wherein a user selects the key type;

selecting a bit length;

generating a key, the generated key having the selected key type and the selected bit length, the step of generating a key being performed in at least one way selected from a group of ways consisting of: 1) sampling an output of a random number generator to assemble a desired length data encryption key (DEK); 2) sampling an output of a random number generator to assemble a desired length key encryption key (KEK); 3) performing a Diffie-Hellman g^{xy} exponentiation in order to arrive at a shared secret value; 4) deriving a symmetrical secret key by hashing an application supplied password or passphrase; 5) transforming an existing key; and 6) importing an unencrypted (RED) key provided by the application; and

representing the generated key in one of an external form and an internal form, the method of managing encryption keys supporting an internally generated storage variable, a local storage variable and a user application generated KEK.--.